

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
APPLICATION FOR PATENT

5           **APPARATUS AND METHOD FOR ACCESSING MATERIAL USING AN ENTITY  
LOCKED SECURE REGISTRY**

Inventor: David C. Collier, and  
Robert J. Fenney

10

**CROSS REFERENCE TO RELATED APPLICATIONS**

This application claims priority to U.S.  
provisional application S.N. 60/\_\_\_\_ filed October 18,  
2001 under Express Mail Label EL337672351US.

15

**FIELD OF THE INVENTION**

The present invention generally relates to material  
accessing techniques and in particular, to an apparatus and  
method for accessing material using an entity-locked secure  
20       registry.

**BACKGROUND OF THE INVENTION**

Providers of material demand compensation for the  
use of their material or content. Unauthorized use cheats  
25       these providers of their due compensation. Therefore,  
techniques for preventing such unauthorized use have been and  
continue to be developed.

Transfers of material are commonly performed over a  
secure channel such as those using authentication and key  
30       exchange techniques. Once the material is transferred, a  
recipient system should be secure so that authorized use,  
copying and/or transferring of the material is controlled and

unauthorized use, copying and transferring of the material is prevented.

**OBJECTS AND SUMMARY OF THE INVENTION**

5 Accordingly, two objects of the present invention are to provide an apparatus and method for accessing material that is secure.

10 Other objects are to provide an apparatus and method for accessing material that carefully controls authorized use, copying or transferring of material.

Still other objects are to provide an apparatus and method for accessing material that prevents or discourages unauthorized use, copying and transferring of material.

15 These and additional objects are accomplished by the various aspects of the present invention wherein briefly stated, one aspect is an apparatus for accessing material, comprising: a secure registry encrypted with a registry key and storing another key useful for decrypting material; and a control module configured to decrypt the secure registry  
20 using the registry key for retrieval of the another key if a correct entity identification is received.

Another aspect is a method for accessing material, comprising: decrypting a secure registry with a registry key; retrieving another key from said decrypted secure registry;  
25 and decrypting encrypted material using said another key to access said material.

Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiments,  
30 which description should be taken in conjunction with the accompanying drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS**

**FIG. 1** illustrates, as an example, a host including an apparatus for accessing material in a file using an entity-locked secure registry, utilizing aspects of the present invention.

**FIG. 2** illustrates, as an example, a system including an apparatus for accessing material in streaming media using an entity-locked secure registry, utilizing aspects of the present invention.

**FIGS. 3~9** illustrate, as examples, various hosts and systems including an apparatus for accessing material using an entity-locked secure registry, utilizing aspects of the present invention.

**FIGS. 10~14** illustrate, as examples, various methods for accessing material, utilizing aspects of the present invention.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT**

As used herein: the terms "audio-visual content" or "A/V content" includes audio, visual and other multimedia content including motion pictures, music, the spoken word, photos, and printed text; "material" and "content" may be used interchangeably, and includes A/V and other distributed content including computer programs or software; and "proprietary material" means material protected by contract or intellectual property law.

**FIG. 1** illustrates, as an example, a host **101** including a control module **104**, an encrypted material **105**, and an entity-locked secure registry **106** that stores access and other information for the encrypted material **105**. Also

included in the host **101** are a control module license manager **107**, and a sensed entity identification ("SE ID") **108** preferably provided by a corresponding entity in response to a request from the control module **104**. The host **101** may be a  
5 personal computer, an entertainment unit such as a set-top box and television set, a network appliance, a wireless communicating device such as a personal digital assistant ("PDA") or other type of electronic device or system with adequate memory and computational power.

10           The sensed entity ID **108** uniquely identifies an entity associated with the secure registry **106**. The entity may be the host **101**, a portable hardware device connectable to the host **101**, or a user of the host **101**. In the case where the entity is the host **101**, the sensed entity ID **108**  
15 is, for examples, a manufacturer's assigned serial number such as for a computer ID, a network interface card ID or a hard disk drive ID. Where the entity is a portable hardware device connectable to the host **101**, the sensed entity ID **108** is, for examples, a smart card ID, a dongle, or a content storage unit (e.g., optical media) ID. On the other hand, in  
20 the case where the entity is a user of the host **101**, the sensed entity ID **108** is, for examples, a credit card number of the user or a conventional user ID entered into an input device, such as a keyboard, by a user of the host **101**, or a  
25 biometrics ID of the user such as the user's fingerprint or speech sensed by a biometrics device coupled to the host **101**.

          The control module **104** includes a registry key (KR) module **109**, encryption module **110**, and decryption module **111**. The control module **104** is preferably implemented as a  
30 computer program running on a processor included in the host **101**. Alternatively, it is implemented as one or more cooperative circuits, or a combination of hardware, software

and/or firmware in a conventional manner. The control module **104** is preferably license-locked to the host **101** using a control module license manager **107** comprising commercially available software such as FLEXlm®, a product of GLOBEtrrotter Software, Inc., a Macrovision company. Alternatively, it is license-locked to another entity such as a portable hardware device connectable to the host **101**, or a user of the host **101**. The registry key (KR) module **109** provides a registry key (KR) for decrypting the secure registry **106**, and encrypting the decrypted version of the secure registry **106**. The encryption module **110** and decryption module **111** respectively perform conventional encryption and decryption functions.

The encrypted material **105** comprises, for example, A/V or other content or proprietary material that has been encrypted for security purposes with at least one content key (KC). Although the decryption module **111** may decrypt the encrypted material **105** with the at least one content key (KC) in order for a user of the host **101** to use the material according to authorized usage rights, preferably, such decryption is performed in a plug-in module to a content player. In this latter case, the control module **104** securely transmits the at least one content key (KC) and relevant terms of a license to the plug-in module to facilitate content decryption and usage. Encrypted material **105** may be stored in host **101** or may be accessed from an inserted media storage unit such as optical media (e.g., CD or DVD media).

The secure registry **106** stores in records, such as record#1 **112** and/or record#2 **113**, access and other information for the encrypted material **105**, such as one or more keys that are useful for decrypting the encrypted material **105** and usage rights taking the form of a license

defining how the decrypted version of the encrypted material **105** may be used. In one embodiment, the at least one content key (KC) used to decrypt the encrypted material **105** is stored in the secure registry **106**. In another embodiment where the  
5 at least one content key (KC) is stored with or separate from the encrypted material **105** and encrypted with at least one license key (KL), the at least one license key (KL) is included in the secure registry **106** instead. Other information that may be stored in the secure registry **106**  
10 include confidential information particular to the host **101** or a user of the host **101**, such as one or more private keys (KUP) and/or other cryptographic secrets. The secure registry **106** is referred to as being "secure", because, among other things, it is maintained in an encrypted state except for a  
15 temporary period when a decrypted version of it is being used. It is also referred to as being "entity-locked", because a registry key (KR) that is associated with the sensed entity ID **108** is used to generate a decrypted version of it in system or other temporary memory of the host **101** so  
20 that the decrypted version may be used, if the sensed entity ID **108** matches a reference entity ID stored in the secure registry **106** or retrieved from the registry key module **109** or provided by the control module license manager **107**. Although it is possible that any one or all of the control module **104**,  
25 encrypted material **105** and secure registry **106** may be inappropriately copied or transferred, the examples described in the various apparatuses and methods herein prevent these from being effectively used by another entity other than the one that the secure registry **106** is locked to or associated  
30 with.

**FIG. 2** illustrates a system including a host **201** and a server **202** communicating through a communication medium

203 such as the Internet. The host 201 is similarly configured as the host 101 of FIG. 1, except that in this case, instead of storing an encrypted material file such as encrypted material 105 in FIG. 1, it receives a copy of 5 encrypted material 205 stored on the server 202 as streaming media, such as in an MPEG-4 bit stream, over the communication medium 203. The control module 104 prepares for receiving the streaming material by first retrieving the registry key (KR) from the registry key module 109, and 10 decrypting the secure registry 106 with the registry key (KR) and retrieving one or more keys to access the encrypted material from the decrypted version of the secure registry 106 if a correct entity identification is received. The control module 104 determines whether or not the correct 15 entity identification is received by comparing a reference entity ID against the sensed entity ID 108. If they match, then the control module 104 determines that the correct entity identification has been received. Processing of the received streaming media is then performed "on-the-fly" by 20 the control module 104 (or a media player including a plug-in module) decrypting the received streaming media and using it according to usage rights also retrieved from the decrypted version of the secure registry 106.

FIG. 3 illustrates another system including a host 25 301 and a server 302 communicating through a communication medium 303. The host 301 is one embodiment of the host 101 of FIG. 1, in which, the registry key (KR) module 109 comprises a replaceable software module ("RSM") 304 providing a registry key (KR) for decrypting the secure registry 106, 30 and a compare module 305 for comparing the sensed entity ID ("SE ID") 108 against a reference entity identification ("RE ID") stored in a record 306 of the secure registry 106. The

replaceable software module **304** is preferably provided by the remote server **302**, for examples, as a dynamic link library module (".**dll**"), Java applet, Window COM object, or Active X object with the registry key (KR) included as data therein.

- 5 It is referred to as being "replaceable," because it is separately downloadable from the rest of the control module that is referred to herein as the control program. Once downloaded, it can be immediately used by the control program. Although the reference entity ID is stored in the 10 secure registry **106** in this example, alternatively and preferably, it is provided along with the registry key (KR) in the replaceable software module **304** after the server providing the replaceable software module **304** to the host **301** receives the sensed entity ID **108** directly or indirectly from 15 the host **301**.

Before a user of the host **301** is allowed to use the encrypted material **105**, the control module **104** first reads the registry key (KR) from the replaceable software module **304**, "opens" the secure registry **106** by generating a 20 decrypted version of it in memory using decryption module **111**, reads the reference entity ID from record **306** in the decrypted version of the secure registry **106**, reads the sensed entity ID **108**, and compares the reference and sensed entity ID's using compare module **305**.

- 25 If the reference and sensed entity ID's match, then the user is allowed to use the encrypted material **105** according to usage rights that are defined, for example, in a content license stored in record **307** of the decrypted version of the secure registry **106**. To allow usage of the encrypted 30 material **105**, the control module **104** first retrieves a key from the decrypted version of the secure registry **106**. In this example, the retrieved key is at least one content key

(KC) that is used by the decryption module **111** to generate a decrypted version of the encrypted material **105** for use.

On the other hand, if the reference and sensed entity ID's do not match, then the user is not allowed to use  
5 the encrypted material **105**. In particular, in such case, the control module **104** (or a plug-in to a media or content player) does not decrypt the encrypted material **105**, and instead, displays an error message on the host screen indicating such failure to a user of the host **301**. A log of  
10 the failed attempt may also be kept in a secret location.

It is prudent to change the registry key (KR) from time to time for security purposes. To do so, the remote server **302** first transmits a replaceable software module such as **304** that is linked to the control module **104**. The  
15 replaceable software module provides two registry keys in this case, a new registry key and the old registry key. The old registry key is used to generate a decrypted version of the secure registry **106**, and the new registry key is used to encrypt the decrypted version. The original secure registry  
20 **106** is then replaced with the newly encrypted version. Subsequent decrypting of the secure registry would then be performed using the new registry key.

**FIG. 4** illustrates a system including a host **401** and a server **402** communicating through a communication medium  
25 **403**. The host **401** is another embodiment of the host **101** of **FIG. 1**, in which, the registry key (KR) module **109** is integrated directly into the binary executable code of the control module **104** such that if either the registry key (KR) or reference entity ID ("RE ID") included therein is  
30 subsequently changed, the entire control module **104** would have to be replaced. The registry key (KR) module **109** in

this example also includes a compare module **405** for comparing the sensed entity ID ("SE ID") **108** against the reference entity ID. The remote server **402** provided the binary executable code of the control module **104** to the host **401** after receiving information of the sensed entity ID **108** from the host **401**. Access to the encrypted material **105** is then performed in a similar manner as described in reference to **FIG. 3**. Although the reference entity ID is integrated into the binary executable code of the control module **104** in this example, it could also be stored in one of the records of the secure registry **106**, as in the host **301** of **FIG. 3**.

**FIG. 5** illustrates a system including a host **501** and a server **502** communicating through a communication medium **503**. The host **501** is another embodiment of the host **101** of **FIG. 1**. In the host **501**, the registry key (KR) module **109** includes a replaceable software module **504** such as the replaceable software module **304** in **FIG. 3**. However, a reference entity ID **506** and compare module **505** are located on the remote server **502**, instead of on the host **501**. As in the prior examples, the reference entity ID **506** indicates the entity that is authorized to access contents of the secure registry **106**, and is provided as the sensed entity ID **108** to the server **502** at the time of licensing the encrypted material **105** for use by the entity. In one embodiment, the entity itself provides the sensed entity ID **108** to the server **502** so as to define the reference entity ID **506**. In another embodiment, an intermediary such as a separate licensing server provides the sensed entity ID **108** to the server **502**.

When a user of the host **501** requests access to the encrypted material **105**, the control module **104** transmits the sensed entity ID **108** to the server **502**. The server **502** then

compares the received sensed entity ID **108** against the reference entity ID **506** using the compare module **505**. If the reference and sensed entity IDs match, then the server **502** sends a transaction approval to the host **501**. The control 5 module **104** of the host **501** then reads the registry key (KR) provided in the replaceable software module **504**, decrypts the secure registry **106** with the registry key (KR), retrieves at least one content key (KC) stored in a record **304** of the secure registry **106**, and uses the at least one content key 10 (KC) to decrypt the encrypted material **105**.

In a variation of the host **501**, the registry key (KR) is integrated directly into the binary executable code of the control module **104** such as described in reference to FIG. 4, instead of in the replaceable software module **504**.

15 In all other respects, configuration and use of this variation is generally the same as the host **501** operating in cooperation with the server **502**.

FIG. 6 illustrates a host **601** that is another embodiment of the host **101** of FIG. 1. In the host **601**, the registry key (KR) module **109** comprises a registry key generator **602** that generates the registry key (KR) from the sensed entity ID **108** preferably in such a fashion that the generated registry key (KR) is unique to the sensed entity ID **108** (i.e., no other sensed entity ID generates the same 20 registry key as the sensed entity ID **108**) and repeatable (i.e., the same registry key output is generated each time for the same sensed entity ID input). In one embodiment, the registry key generator **602** is implemented as a pseudo-random number generator that generates the registry key (KR) as a 25 pseudo-random number from the sensed entity ID **108** that is provided as a seed to the pseudo-random number generator. 30

For security reasons, the algorithm for the pseudo-random number generator is kept secret.

Since the secure registry **106** is encrypted and decrypted with the registry key (KR) generated from the sensed entity ID **108**, any other sensed entity ID (different than the sensed entity ID **108**) provided to the registry key generator **602** will not generate a registry key (KR) capable of decrypting the secure registry **106** to read its contents. Consequently, access keys and other information related to the encrypted material **106**, that are stored in the secure registry **106**, are not available to an unauthorized entity. Although implementation of the registry key generator **602** adds some complexity to the registry key module **109**, the elimination of a compare module such as **305** in **FIG. 3**, helps compensate somewhat for such added complexity.

**FIG. 7** illustrates a host **701** that is another embodiment of the host **101** of **FIG. 1**. In the host **701**, the registry key (KR) module **109** includes an embedded key (KR') **702** and a mixer **703** that generates the registry key (KR) by mixing the embedded key (KR') **702** and a sensed entity ID **108** (or a pseudo-random number generated from the sensed entity ID **108**) preferably in such a fashion that the generated registry key (KR) is unique to the sensed entity ID **108** (i.e., no other sensed entity ID generates the same registry key as the sensed entity ID **108**) and repeatable (i.e., the same registry key output is generated each time for the same sensed entity ID input). In one embodiment, the embedded key (KR') **702** is provided in a replaceable software module such as **304** in **FIG. 3** to the host **701** from a remote server. In another embodiment, the embedded key (KR') **702** is integrated directly into the binary executable code of the control

module **104**, which is provided to the host **701** from a remote server. In both embodiments, the remote server can effectively change the registry key (KR) by providing a new and old embedded key in basically the same manner as

5 described in reference to **FIG. 3.**

**FIG. 8** illustrates a host **801** that is another embodiment of the host **101** of **FIG. 1**. In the host **801**, the at least one content key (KC) used to decrypt the encrypted material **105** is itself, encrypted with at least one license key (KL) and provided in a file **802** along with the encrypted material **105** by a remote server. The at least one license key (KL), as its name suggests, is associated with a license providing usage rights to the encrypted material **105**. The at least one license key (KL) and the license are stored, for example, in a record **803** of the secure registry **106**, so that a user of the host **801** may only access the encrypted material **105** after the at least one license key (KL) has been retrieved from the secure registry **106**, the decryption module **111** has decrypted the at least one content key (KC) using the retrieved at least one license key (KL), and the encrypted material **105** has been decrypted using the at least one content key (KC). The control module **104** (or plug-in to a media or content player) that decrypts the encrypted material **105** then controls usage of the decrypted version of the encrypted material **105** according to its corresponding content license retrieved from the secure registry **106**. Access to the secure registry **106** for retrieval of the at least one license key (KL) and the content license is performed in the same manner as described, for example, in reference to **FIG.**

25 **1**, and other examples described herein as applicable.

30

2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
689  
690  
691  
692  
693  
694  
695  
696  
697  
697  
698  
699  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
789  
790  
791  
792  
793  
794  
795  
796  
797  
797  
798  
799  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
889  
890  
891  
892  
893  
894  
895  
896  
897  
897  
898  
899  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
989  
990  
991  
992  
993  
994  
995  
995  
996  
997  
997  
998  
999  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1095  
1096  
1097  
1097  
1098  
1099  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1195  
1196  
1197  
1197  
1198  
1199  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1295  
1296  
1297  
1297  
1298  
1299  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1395  
1396  
1397  
1397  
1398  
1399  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1495  
1496  
1497  
1497  
1498  
1499  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1595  
1596  
1597  
1597  
1598  
1599  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1695  
1696  
1697  
1697  
1698  
1699  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1795  
1796  
1797  
1797  
1798  
1799  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1895  
1896  
1897  
1897  
1898  
1899  
1899  
1

control module decrypts a secure registry on the host with the registry key to generate a decrypted version of the secure registry. In **1005**, the control module receives or retrieves a reference entity identification ("ID"). In **1006**,  
5 the control module compares the sensed entity ID with the reference entity ID to determine whether the IDs match. If they do not match (i.e., are different), then in **1007**, the control module terminates the transaction.

On the other hand, if they do match (i.e., are the same), then in **1008**, the control module reads or retrieves at least one key from the decrypted version of the secure registry, and in **1009**, the control module reads or retrieves usage rights contained in a license from the decrypted version of the secure registry. The retrieved at least one key in this case may be at least one content key that is used to decrypt the requested encrypted material, or it may be at least one license key that is used to decrypt an encrypted at least one content key, which in turn, is used to decrypt the requested encrypted material. In **1010**, the requested  
15 encrypted material is decrypted using the at least one key, and in **1011**, the user is allowed to use the decrypted material according to the terms of the license. The control module may perform **1010** and **1011**, or a plug-in module to a media or content player may perform **1010** and **1011** after  
20 securely receiving the at least one retrieved key from the control module and the encrypted material from the control module or other source.  
25

**FIG. 11** illustrates a flow diagram of a method for accessing material that is implemented, for example, by the host described in reference to **FIG. 4**. In **1101**, a control module on a host receives a request from a user of the host to use material that is stored in encrypted form on the host.

In 1102, in response to such request, the control module either receives after requesting from an entity or retrieves from storage in the entity, a sensed entity ID. In 1103, the control module receives or retrieves a reference entity ID.

- 5 In 1104, the control module compares the sensed entity ID with the reference entity ID to determine whether the IDs match. If they do not match (i.e., are different), then in 1105, the control module terminates the transaction.

On the other hand, if they do match (i.e., are the same), then in 1106, the control module reads a registry key preferably provided by a registry key module. In 1107, the control module decrypts a secure registry on the host with the registry key to generate a decrypted version of the secure registry. In 1108, the control module reads or retrieves at least one key from the decrypted version of the secure registry, and in 1109, the control module reads or retrieves usage rights contained in a license from the decrypted version of the secure registry. The retrieved at least one key in this case may be at least one content key that is used to decrypt the requested encrypted material, or it may be at least one license key that is used to decrypt an encrypted at least one content key, which in turn, is used to decrypt the requested encrypted material. In 1110, the requested encrypted material is decrypted using the at least one key, and in 1111, the user is allowed to use the decrypted material according to the terms of the license. The control module may perform 1110 and 1111, or a plug-in module to a media or content player may perform 1110 and 1111 after securely receiving the at least one retrieved key from 30 the control module and the encrypted material from the control module or other source.

**FIG. 12** illustrates a flow diagram of a method for accessing material that is implemented, for example, by the system described in reference to **FIG. 5**. In **1201**, a control module on a host receives a request from a user of the host to use material that is stored in encrypted form on the host. In **1202**, the control module next receives a sensed entity ID uniquely corresponding to either the host or the user of the host. In **1203**, the control module transmits the sensed entity ID to a remote server. In **1204**, the control module receives either an approval or disapproval for the transaction from the remote server. Approval is received if the sensed entity ID matches with a reference entity ID stored on the remote server. Conversely, a disapproval of the transaction is received if there is no match.

In **1205**, the control module terminates the transaction if a disapproval of the transaction is received. On the other hand, if approval is received, in **1206**, the control module reads a registry key provided by a registry key module. In **1207**, the control module decrypts a secure registry on the host with the registry key to generate a decrypted version of the secure registry. In **1208**, the control module reads or retrieves at least one key from the decrypted version of the secure registry that is useful for accessing the encrypted material. In one embodiment, the at least one key is at least one content key (KC) used for decrypting the encrypted material. In another embodiment, the at least one key is at least one license key (KL) used for decrypting an encrypted version of the at least one content key (KC). In **1209**, the control module reads or retrieves usage rights contained in a license from the decrypted version of the secure registry.

In **1210**, the requested encrypted material is decrypted using the retrieved keys. In one embodiment, where the at least one key is at least one content key (KC), the at least one content key (KC) is used to directly decrypt the 5 encrypted material. In another embodiment, where the at least one key is at least one license key (KL), the at least one license key (KL) is used to decrypt the encrypted at least one content key (KC), which in turn, is used to decrypt the encrypted material. In **1211**, the user is allowed to use 10 the decrypted material according to the terms of the license. The control module may perform **1210** and **1211** or a player plug-in may perform them. In the case of the player plug-in performing **1210** and **1211**, the control module first securely transmits the at least one key and the terms of the license 15 to the player plug-in, using, for example, a conventional acknowledgement and key exchange procedure such as Diffie-Hellman.

**FIG. 13** illustrates a flow diagram of a method for accessing material that is implemented, for examples, by the 20 hosts described in reference to **FIGS. 6** and **7**. In **1301**, a control module on a host receives a request from a user of the host to use material that is stored in encrypted form on the host. In **1302**, the control module next receives a sensed entity ID uniquely corresponding to either the host or the 25 user of the host. In **1303**, the control module generates a registry key (KR) using the sensed entity ID. In **1304**, the control module generates a decrypted version of an encrypted secure registry with the registry key (KR). Since the secure registry had been previously encrypted with a registry key 30 (KR) corresponding to the original sensed entity ID, only a registry key generated from the original sensed entity ID is capable of decrypting the secure registry. The original

sensed entity ID is also referred to herein as the reference entity ID.

In 1305, the control module makes a determination whether or not the decryption of the secure registry was successful. In this regard, it is implicit that the sensed entity ID must be the same as the reference entity ID in order for the generated registry key (KR) to successfully decrypt the encrypted secure registry. For this reason, the secure registry is also referred to as being entity-locked.

5 If the decryption was unsuccessful, then in 1306, the control module terminates the transaction. On the other hand, if the decryption was successful, then in 1307, the control module reads or retrieves at least one key from the decrypted version of the encrypted secure registry; in 1308, the control module reads a license including usage rights from the decrypted version of the secure registry; in 1309, the encrypted material is decrypted using the retrieved at least one key; and in 1310, the user is allowed to use the decrypted material according to the terms of the license,

10 wherein 1307~1310 are performed in much the same manner as respectively corresponding 1208~1211 of FIG. 12.

15

20

**FIG. 14** illustrates a flow diagram of a method for accessing material that is implemented, for example, by the system described in reference to **FIG. 9**. In the method, 1401~1407 are performed by a control module in much the same manner as respectively corresponding 1101~1107 of **FIG. 11**. In this method, however, the at least one content key (KC) is encrypted with at least one license key (KL) and provided along with material that is encrypted with the at least one content key to the host. Therefore, in 1408, the control module reads or retrieves the at least one license key (KL) from the decrypted version of the secure registry, and in

25

30

1409, it reads or retrieves usage rights contained in a license from the decrypted version of the secure registry. In 1410 and 1411, the control module then receives the encrypted material and the encrypted at least one content key 5 (KC), for example, in an MPEG-4 bit stream and its corresponding IPMP stream. In 1412~1414, a plug-in module to a media or content player then, preferably, processes the received material "on-the-fly" after securely receiving the at least one license key (KL) and corresponding usage rights 10 from the control module. The plug-in module preferably does this by generating a decrypted version of the encrypted at least one content key (KC) using the at least one license key (KL) in 1412, generating a decrypted version of the encrypted material using the decrypted version of the encrypted at 15 least one content key (KC) in 1413, and allowing the user to use the decrypted version of the encrypted material according to the usage rights in 1414.

In the case where the received encrypted material and encrypted at least one content key (KC) are not processed 20 "on-the-fly", but stored instead in one or more files on the host such as 105 and 802 in FIG. 8, the control module simply processes the stored files according to the method of FIG. 14 without performing 1410 and 1412.

Although the various aspects of the invention have 25 been described with respect to preferred embodiments, it will be understood that the invention is entitled to full protection within the full scope of the appended claims.